
# HERE AT ARRAY NETWORK ON-PREMISES, DDoS DEFENSES IS THE ADS. IT CAN PROVIDE COMPREHENSIVE, MULTI-LAYERED PROTECTION FROM ALL THE ADVANCED DDOS ATTACKS.

Nothing more destructive and complex exists than a DDoS attack. A distributed denial-of-service (DDoS) attack is a malicious attempt to interrupt normal traffic of a targeted server, service or network by devastating the target or its surrounding infrastructure/ organization with a flood of Internet traffic. The DDoS attack is like a traffic jam that clogs up the highway, preventing regular traffic from arriving at its desired destination.

The moment it is deployed out-of-path, traffic streams for the IP addresses under attack are "diverted/ sidetracked" to the ADS. Allowing all the legitimate traffic to pass downstream as ADS surgically mitigates the DDoS attack traffic. And on the other hand, when it is deployed in-line, the ADS detect attacks and mitigates DDoS traffic. In both the deployment modes, extremely low latency and reliable detection and mitigation of attacks are provided, which in turn ensures that the service provider's customers and services are protected from the impact of DDoS.

## Monitor

Easy deployment of ADS in any provider's network creates a win-win situation, as it can scale up to hundreds of Gbps of inspected traffic. When the deployment is in-line, ADS monitors the incoming traffic for signs of DDoS. And when the deployment is out-of-path, the Traffic Analyzer monitors and detects by consuming xFlow data from border, core, or edge routers. Both the methods provide reliable monitoring and detection of DDoS.

## Detect

The core of the ADS is made up of innovative, multi-stage detection engines. To identify both legitimate and attack traffic, all the packets are subjected to a series of analysis, checks, and validations. This includes RFC Checks, Protocol Analysis, Access Control Lists, IP Reputation, Anti-spoofing, L4-L7 Algorithmic Analysis, User Behavior Analysis, Regular Expressions, Fragmentation Controls, Connection, and Rate Limiting.

Together they provide industry-leading precision that protects against all DDoS attacks. The detection engine is optimized frequently, so providers always have the most accurate protection available.

## Mitigate

Regardless of the deployment scenario, once the attack traffic has been identified by ADS, it instantly removes the traffic from the streams it's inspecting. Later, ADS then forward only legitimate traffic to its intended destination. Additionally, the ADS can integrate with Threat Intelligence to remove the traffic from known botnets instantly and query the newest threat intelligence regarding the attackers. The ADS support DDoS attack reporting in real-time that helps to provide valuable information such as attack types, source/ destination IPs, protocols, and more. An integrated web services API can also be used to assist with automated configuration, post-incident reporting, and billing operations.

## Performance. Quality. Value.

The ADS is the ideal solution for service providers to mitigate DDoS attacks against their customers, and their services. No null routes to defeat DDoS attacks is needed once the providers have deployed the ADS. It is available in a range of cost and performance-optimized appliances. ADS has been purpose-built to deliver high quality, scalable mitigation of DDoS attack traffic.

## Highlights & Benefits

ADS defeat DDoS attacks against the customers when deployed in their network. ADS reduces operating expenses for DDoS mitigation by providing increased levels of automation.

- **Multi-Tenant Design:** Domain-specific configurations, learning algorithms, automated mitigation responses, modular architectures, flexible licensing models, and the lowest total cost of ownership (TCO).
- **Reliable, Accurate:** Algorithmic, multi-filter, the rule-based approach provides automated and reliable DDoS mitigation with low false positives and high performance, efficient and intelligent protection from the botnet-based attacks with Threat Intelligence
- **Best-in-Class Performance:** Provides advanced DDoS mitigation for any size service provider that is easy to integrate with your network.
- Scalable Architecture: Supports scalable clusters for both in-line and out-of-path deployment scenarios to meet the needs of any size network.

## Solution Specifications

### DDoS Protection

- Comprehensive, multi-layered protection against the volumetric, application, and web application attacks
- Multi-protocol support and advanced inspection including TCP/UDP/ICMP/ HTTP/HTTPS/DNS/SIP floods, Amplification attacks (NTP/SSDP/SNMP/ DNS/ CHARGEN/Memcached/NetBIOS), fragments floods, connection exhaustion, header manipulation and more
- Integrated with Threat Intelligence

### DDoS Mitigation Algorithms

- RFC Checks
- Black Filter Lists
- White Filter Lists
- GEOIP Filter Lists
- Access Control Lists Filtering
- TCP Regular Expression Filtering
- UDP Regular Expression Filtering
- SYN Check
- ACK Check
- Reflection Amplification Rules
- Port Check
- Connection Exhaustion
- URL-ACK Filter Lists
- Anti-spoofing
- TCP SYN Source IP Rate Limit
- TCP SYN Source Bandwidth Limit
- TCP SYN Time Sequence Check
- TCP Fragment Control
- ICMP Fragment Control
- ICMP Traffic Control
- NS Keyword Checking
- DNS Rate-Limiting
- DNS TCP-BIT Check
- DNS CNAME Check
- DNS Retransmission
- HTTP Keyword Checking
- HTTP Authentication
- HTTP Dynamic Script
- HTTP FCS Check
- HTTP Pattern Matching Check
- HTTP Slow Attack Check
- IP Behavior Analysis
- Trusted Source IP Control
- Empty Connection Check
- HTTPS SSL Connection Control
- HTTPS Authentication
- SIP Authentication
- UDP Payload Check
- UDP Fragment Control
- UDP Packet Length Check
- UDP Traffic Control
- TCP Watermark Check
- UDP Watermark Check
- TCP Pattern Matching
- UDP Pattern Matching
- Protocol ID Check

### Management

- Protocols: HTTP, SNMP, Email, Syslog
- Authentication: Local database, Radius, TACACS+
- API: web services for reporting and automated configuration

### IP Protocols

- Addressing: IPv4/v6
- Routing: BGP, OSPF, RIP, IS-IS, static routing, and PBR
- Datalink and network layer: MPLS, GRE, VLAN (802.1q)

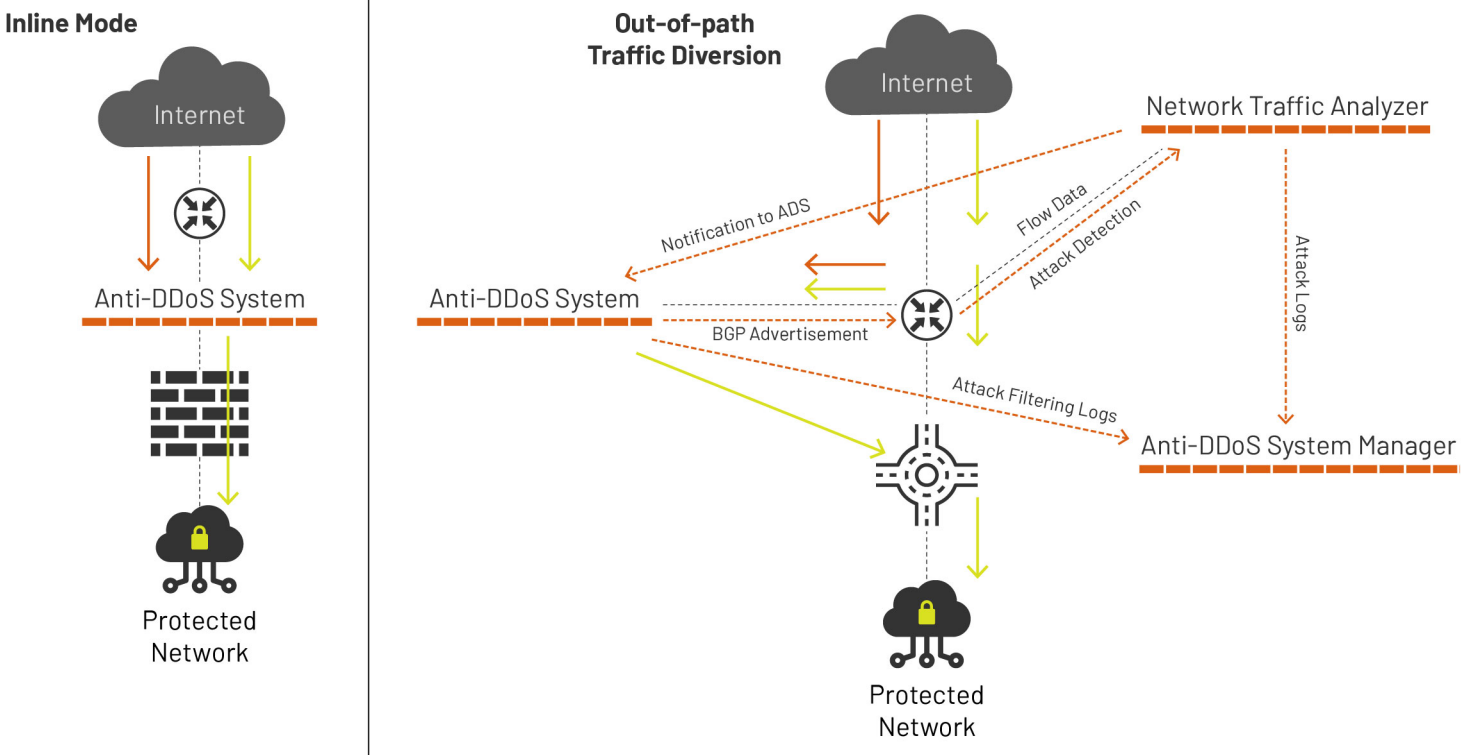
### Reporting

- Real-time and historical reporting of attack types, source/destination IP
- Formatting: XML, PDF, HTML, and Microsoft Word
- Web Service API to support automated configuration and reporting functions

## Deployment Architecture

Currently, ADS devices can be deployed in in path mode or out of path mode based on different network environments. The following sections detail the two modes.

- In path deployment is suitable for enterprises' intranets that are characterized by fewer servers and smaller outgoing bandwidth. In this mode, an ADS device is transparently deployed at the network entry to detect, analyze, and block DDoS attacks.
- Out-of-Path Deployment is suitable To protect crucial businesses of Internet data centers (IDCs), Internet content providers (ICPs), or telecom carriers, ADS devices can be deployed in out-of-path mode, which employs the traffic diversion mechanism. In this mode, an ADS device is deployed at the network entry to collaborate with other routers, performing traffic diversion and injection on one line to protect servers on the network.




The real-time monitoring module provides real-time traffic information and attack information for you to have a full understanding of the current network status.

- Traffic Trend
- Attack Traffic Trend
- Top Ongoing Attack Events
- System Resources
- Collaboration Status
- System Interfaces

ADS support different types of reports: daily report, weekly report, monthly report etc.

## Applications and Security Testing Solutions

| | AVX-5800 | AVX-7800 | AVX-9800 |
|---|---|---|---|
| **Hosted VNF/VAs** | 1, 2, 4 or 8 (16 without performance guarantee) | 2, 4, 8 or 16 | 4, 8, 16 or 32 |
| **Max. L4 Throughput** | 40G | 80G | 160G |
| **Max. SSL TPS** | 40K | 53K | 110K |
| **Max. ECC TPS** | 28K | 38K | 76K |
| **# of CPU Cores** | 4 (8 vCPUs) | 12 (24 vCPUs) | 20 (40 vCPUs) |
| **# of Cryptographic Engines** | 144 | 144 | 288 |
| **RAM** | 64/128 GB | 64/128 GB | 128/256/512 GB |
| **HDD** | 2TB (4TB option) | 2TB (4TB option) | 2TB (4TB option) |
| **1 GbE (copper)** | 4 | 2 | 2 |
| **10 GbE Fiber (SFP+)** | 4 | 8 | 8 or 16 (option) |
| **40 GbE Fiber (QSFP+)** | - | 2 (option) | 4 or 8 (option) |
| **Power Supply** | Dual Power: 100-240VAC, 5-3A, 47-63Hz | Dual Power: 90-264VAC, 10-5A, 47-63Hz | |
| **Typical Power Consumption (W)** | 174 | 281 - 449* | 533 - 581* |
| **BTUs/Hour** | 484 | 788 - 1249* | 1443 - 1550* |
| **Dimensions** | Dual Power: 1U – 17" W x 19.875" D x 1.75" H | Dual Power: 2U – 17" W x 22.5" D x 3.5" H | |
| **Weight** | Dual Power: 19.8 lbs. | Dual Power: 28 lbs. | |
| **Environmental** | Operating Temperature: 0º to 45º C, Humidity: 0% to 90%, Non-condensing | | |
| **Regulatory Compliance** | ICES-003, EN 55024, CISPR 22, AS/NZS 3548, FCC, 47FR part 15 Class A, VCCI-A | | |
| **Safety** | CSA, C/US, CE, IEC 60950-1, CSA 60950-1, EN 60950-1 | | |
| **Support** | Gold, Silver and Bronze Level Support Plans | | |
| **Warranty** | 1 Year Hardware, 90 Days Software | | |


www.array-networks.co.in

**VERSION: APR-2020-REV-A**